TESTIMONY OF

W. Douglas Maughan, Ph.D.
Program Manager, Cyber Security R&D, Science & Technology Directorate
U.S. Department of Homeland Security

Before the
House Committee on Homeland Security
Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

Addressing the Nation's Cyber Security Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action

April 25, 2007

Chairman Langevin, Ranking Member McCaul and Members of the Subcommittee, thank you and good afternoon. Today, I will be sharing with you three important aspects of our work in cyber security research and development in the Department of Homeland Security (DHS) Science and Technology (S&T) Directorate, including our efforts to:

- **Drive security improvements** in existing technologies and emerging systems.

- **Discover solutions to detect, prevent and respond to cyber attacks** on the Nation's critical infrastructure.

- **Deliver new, tested solutions for cyber security threats** and make them widely available to all sectors through technology transfer and other methods.

The S&T Cyber Security R&D goes through the full R&D lifecycle--research, development, testing, evaluation and transition—to produce unclassified solutions that can be implemented for our customers in both the public and private sectors. Therefore, we are able to move these solutions from the lab to real life, so they reach the U.S. businesses and citizens who need them to secure their networks. It means that the results of our research can have an enormous impact in every home and business in the United States, as well as throughout our government and the world. In the past three years alone, the DHS Science and Technology Directorate has funded research that today is realized in more than 10 open-source and commercial products that provide capabilities such as: secure thumb drives, root kit detection, worm and distributed denial of service detection, defenses against phishing, network vulnerability assessment, software analysis, and security for process control systems.

Cyber threats pose an ever-growing risk to our national and economic security. We face enormous challenges in our ability to meet or even anticipate those threats. Today, I hope to describe briefly for you: the scope of the problem; and the positive steps we are taking to drive, discover and deliver new solutions.

The events of September 11, 2001, made clear that the security of our Nation and our economy are intertwined. The majority of government communications utilize private-sector networks, including critical infrastructures -- such as information technology, communications, financial services, electricity, and oil and gas systems. These networks have proven interdependencies that are critical to response capabilities as well as business operations. The systems of these sectors have converged and are interconnected. For example, if the electrical grids fail, that failure impacts the communications systems, which in turn can hamper financial networks.

The Internet connects all other networks, including our Nation's critical infrastructure. It has become the central nervous system for our government, our citizens and our industries. When it is attacked, the effects can ripple far and wide. Although the Internet was developed to provide "essential minimum communications" in the event of a nuclear attack, it was not designed with security in mind. Thus, the technology that is deployed over most of the Internet today has vulnerabilities that can be exploited, endangering all the connecting networks, including our critical infrastructures.

Beyond the Internet, few of the technologies we use every day are adequately protected against malicious attacks. Cell phones, PDAs, and wireless networks are vulnerable, as are the supervisory control and data acquisition (SCADA) systems underlying our critical infrastructure. Attacks on these technologies have forced us into a defensive posture, and the financial costs are significant. Attackers can reach our business and government systems through the maze of networks connected by the Internet.

A 2004 Congressional Research Service (CRS) report stated that cyber attacks on publicly traded firms resulted in losses of 1 percent to 5 percent on the firms' stock price in the days following an attack. For the average New York Stock Exchange company, this means shareholder losses in the range of $50 million to $200 million. CRS reported that total losses worldwide in 2003 attributed to viruses, worms, and all other hostile digital attacks were $226 billion. These attacks can come from rogue actors (such as script kiddies, disgruntled employees, and organized crime), terrorists, insiders, and other nation states.

But it is not just companies and governments at risk: Our citizens also are vulnerable. Government action can help protect U.S. consumers who, in many cases, cannot adequately protect themselves from threats that come from our cyber infrastructure. Countering these threats requires the deployment of new technologies across the global infrastructure.

Americans make extensive use of the Internet. March 2007 global statistics indicate there are more than 210 million Americans – 70 percent of our total population – using the Internet. On their private computers, our citizens are targeted by viruses, worms, and phishing schemes. Their computers may be used as launching pads for attacks against other systems, unbeknownst to the computer owner. To date, more than 150 million records containing personally identifiable information have been exposed since January 2005, according to the Privacy Rights Clearinghouse.

According to a 2005 *Consumer Reports* survey in the U.S., 86 percent of Americans who go online have made at least one behavior change due to fears about online theft. 29 percent have cut back on shopping online, and another 25 percent have stopped shopping online altogether. A 2006 survey from the Cyber Security Industry Alliance (CSIA) found that Internet users who do shop online indicate that they spend an average of $116 per month per person – an estimated $8 billion per month in total -- but that half of all users avoid making purchases because of fear of identify theft or compromise of financial information.

Indeed, citizens want the Federal government to bring forward cyber security protections. A 2005 survey of U.S. voters – both Internet users and non-users -- conducted by CSIA found that respondents look to the U.S. government to help with cyber security issues. Sixty-five percent of the respondents indicated that the government needs to do more to protect information and systems.

In fact, the Department of Homeland Security's Science and Technology Cyber Security program serves all of these customers, which include both DHS internal components and private sector entities: Cyber Security and Communications (which includes the National Cyber Security

Division and the National Communications System), U. S. Secret Service, DHS Chief Information Officer (CIO), Internet infrastructure owners and operators, critical infrastructure providers, and the information security research community. The Directorate leads the government's charge in funding cyber security research and development that results in deployable security solutions, as directed by the President in the *National Strategy to Secure Cyberspace*. Our research and development funding is targeting the critical problems that threaten the integrity, availability, and reliability of our networks. We provide solutions and research resources that advance our understanding of cyber security risks. Our goals are:

- To protect our national and economic security interests and secure our homeland.

- To enable the government, industry, and citizens to make better-informed decisions about cyber security risks.

- To provide the resources needed to counter and mitigate these risks.

The United States played a formative role in the Internet's creation, and is home to ten of the thirteen root servers that control the communications flowing over the Internet. However, today's security vulnerabilities cannot be addressed in isolation. Today, there are 243 countries connected to the Internet and approximately 1.2 billion online users worldwide. It is a global problem that affects governments, businesses, and citizens. To get this important work done, the S&T Cyber Security R&D program carefully collaborates with private industry, Federal agencies and other governmental entities, and private-sector partners in other nations, reflecting the truly global nature of the Internet.

There are legal issues and international coordination issues that need to be addressed, but there are also complex technical problems that need to be solved. The price tag for this research and development is high, but it is minimal compared to the cost of cyber attacks today. Let me restate for the members of the Subcommittee that worldwide cyber attacks were estimated by CRS at a cost of $226 billion in 2003. The cost impact is most certainly higher today. The Department of Homeland Security's Science and Technology Directorate's cyber security research and development budget totaled $13 million in FY 2007 and the President has requested $14.8 million for Fiscal Year 2008.

Today, I'm going to discuss three important areas where we are:

- Driving security improvements to address critical weaknesses in the Internet's infrastructure

- Discovering new solutions for emerging cyber security threats, by incubating ideas and innovation in safe testing environments and public-private partnerships

- Delivering new technologies tested in a real-world environment and making them widely available for real-world users in all sectors

I also will describe for you those research areas identified in concert with our customers that are ongoing priorities which we will continue to address in FY2007, FY 2008 and beyond:

Driving Security Improvements to Address Critical Weaknesses

The Department of Homeland Security's Science and Technology Directorate is leading efforts to secure two of the Nation's major technology vulnerabilities: security weaknesses in the Internet's domain name system, or DNS, and vulnerabilities in the Internet routing system. Attacks against these two parts of the Internet infrastructure are particularly insidious because computer users cannot detect them. Attack traffic is estimated to have skyrocketed 150-fold since 2000.

Both domain name system and routing vulnerabilities can deny service to small or large portions of the Internet, make tracking and tracing Internet communications very difficult, or allow communications to be redirected without the user's knowledge. In the dot-com and dot-net domains alone, domain name queries are made an average of 24 billion times a day, yet Internet users have no guarantee that they will reach the Web site they want when they enter its address in a browser. Symantec's most recent *Internet Security Threat Report* notes that, in the first six months of 2006, spam made up 54 percent of all monitored e-mail traffic. Much of that spam takes advantage of weaknesses in the routing system, and uses it to mask spammers' identities, making it difficult, if not impossible, to track them down and prosecute them.

U.S. government leadership in addressing these critical vulnerabilities is essential, and the President's *National Strategy* calls on DHS to drive the efforts to bring solutions forward. By working in a collaborative effort across Federal agencies, private industry, and global Internet owners and operators, the DHS Science and Technology Directorate has made progress toward addressing these problems. In cooperation with NIST and the Department of Commerce, our Directorate leads the effort to develop domain name security extensions (DNSSEC), and we work with international counterparts and key technical groups to develop improvements to the standards that govern addressing and routing.

Both of these infrastructure security problems have, or soon will have, solutions driven by our government's leadership. The remaining challenge lies in convincing the many owners and users of the Internet to *deploy* them, from private industry and foreign governments to our own state, local and federal agencies in the U.S. New requirements under the Federal Information Security Management Act (FISMA) call for DNS security extensions to be deployed across all federal agencies and their contractors. A few other countries, notably Sweden, have already deployed the important DNS security solution.

The private sector also is starting to follow the government's lead. Two major corporations working in software and information security also have announced plans to include DNS security extensions in their products going forward. Microsoft, which supplies the operating system for the vast majority of the U.S. government's desktop computers, will include the new DNS security protocols in a forthcoming upgrade of its software. VeriSign also has announced that it will include the DNS security protocols as part of an expansion that will enable it to handle more than four trillion domain name system queries per day. Many more government agencies and industries must take similar steps if we are to secure the Internet infrastructure.

The government has a special role to play in coordinating the deployment of these solutions. The S&T Cyber Security R&D program is positioned to carry this work forward. Building on our research and development efforts, the government can play an even greater leadership role by taking steps to ensure the government-wide deployment of DNS security extensions and secure routing technologies, when available.

Discovering New Solutions for Emerging Cyber Security Threats

We cannot focus solely on known problems. One of the most important aspects of cyber security R&D involves understanding new threats and risks, and discovering solutions that will help us protect our Nation's cyber infrastructure. Because the research we conduct is unclassified, it can be deployed by the private sector. The S&T Cyber Security R&D program funds two efforts that provide a safe environment for cyber security research. Using small business innovation research funding and other programs in our Directorate, we also provide funding that helps bring forward the next generation of cyber solutions so they can be adapted for wider use against emerging threats. With more than 30 small business innovation research grants in progress today, as well as other funds, we are incubating ideas that emanate from small companies and devising solutions for emerging problems that will affect major sectors.

The need to create, test, and learn from potential threats poses a problem in itself. We want to test threats to the Internet, but if we conduct such R&D testing on the actual Internet, we could inadvertently put it at risk. To provide scientifically rigorous testing for next-generation cyber defense technologies, the DHS Science and Technology Directorate funds a cyber security testing environment, comprised of a test network, and test data sets containing real-traffic data.

The network, called the Cyber Defense Technology Experiment Research Testbed Program, or DETER, offers cyber security researchers a way to run experiments on a secure "virtual Internet," keeping the Internet safe. This testbed was jointly funded with NSF and now more than 50 organizations from more than 20 states --which includes major research universities, national laboratories and high-tech companies -- are using the DETER test bed. The test bed began with 200 systems, and has been increasing by 200 per year with a goal of 1,000 systems spread across six sites by FY09.

In addition to a test network, researchers need data sets to use for testing their solutions. These data sets, however, have not existed, impeding effective testing of potential technologies. For example, the most widely used data source today was created in 1998 by the Defense Advanced Research Projects Agency (DARPA). Traffic data that is nine years old cannot be used to analyze today's attacks, viruses, malicious code, and traffic patterns.

The S&T Cyber Security R&D program created and funded the Protected Repository for Defense of Infrastructure Against Cyber Threats, or PREDICT program, to serve as a repository for a collection of datasets that can be used for testing new ideas and solutions. PREDICT provides datasets for information security testing and for the evaluation of maturing network technologies, to help advance them toward commercial development. The PREDICT data repository also is designed to hold datasets which can be collected from private companies, without violating their proprietary concerns, for sharing with network security researchers. The PREDICT program has taken groundbreaking steps to ensure that data privacy is protected, including reviewing the project with major privacy organizations.

As I noted earlier, another critical area of focus for the DHS Science and Technology Directorate is the development and deployment of the next generation of cyber security technologies that we need if we are to effectively face emerging threats to our Nation's critical infrastructure. We solicit research proposals for new technologies, prototype technologies and mature technologies, so that our investment yields solutions that are poised for commercial adoption. Under the first round of this research funding effort, we awarded $13.8 million. The $13.8 million funded projects in 12 states: California, Delaware, Georgia, Massachusetts, Maryland, Michigan, Minnesota, New Hampshire, New Jersey, New York, Texas, and Virginia.

Let me give you some examples of projects we've funded in this area:

- In California, Stanford University researchers are identifying and fixing serious bugs in open source code for freely available software. Widely used, open source software makes up a large part of the Nation's cyber-infrastructure, and this effort has lead to tools that are available through a commercial company named Coverity, located in San Francisco and Boston.

- In Ann Arbor, the University of Michigan's researchers are working on a secure crisis response system using handheld devices. Using low-cost disposable handheld devices, first responders will be able to have a secure mobile coordination and syndication channel -- a lightweight means for interagency communication and coordination using industry-standard wireless and cell phone technologies, while keeping data transmission secure. This project partners with Lucent Technologies for commercial deployment.

- At Dartmouth College, researchers are analyzing wireless traffic to detect and respond to attacks on a WiFi network. The project is working with Aruba Networks of Sunnyvale, California, a very large wireless vendor in the United States, to develop and deploy an operational prototype and evaluate it with real-time users.

Additionally, we are partnering with the financial sector to assess the economic impact that a cyber security attack might have on individual enterprises, and developing tools to help financial companies assess and manage the risks that such a disruption of service could create.

Working with companies like Citigroup and Pershing LLC, a brokerage subsidiary of the Bank of New York, we have created a prototype of a risk management tool for the finance sector. It is designed to help create a computer simulation of a financial enterprise and its value chains, and how they interconnect with other institutions. Once it is finalized, the tool will allow them to create and run disruption scenarios tailored to their business operations, using their own proprietary data as well as generic data for the rest of the financial sector. In this way, they can find out specifically how a cyber security event or attack will affect their business, using real-time sector data while protecting their companies' proprietary data.

I want to underscore the special role that government funding has played in developing this prototype. No single financial company would build such a tool and share it with competitors; however, because of support from our Directorate, the entire financial sector will be able to assess and protect itself against emerging cyber security threats, protecting our Nation's critical infrastructure.

Delivering New, Tested Technologies Widely Available for All Sectors

New cyber security solutions do not appear in products automatically. Technology transfer from the lab to the marketplace is a vital and unique aspect of our Directorate's cyber security R&D effort. The S&T Cyber Security R&D program extends beyond knowledge and the proof of whether security solutions are feasible. Based on this foundation of rigorous research and development, we create public-private partnerships, acting as a catalyst to deliver new, tested technology solutions for cyber security threats and make them widely available for use in all sectors.

One important test we have conducted focused on handheld wireless devices, like the BlackBerry and other mobile data communications devices. These devices are expected to proliferate within government agencies. According to a 2005 survey in *Government Computing News*, 40 percent of all government managers report that they use some form of handheld wireless device. Hundreds of thousands of these devices are currently employed in government business, yet today, most mobile data architectures cannot sufficiently assure high-level government security.

To address those issues, and to identify the needs in infrastructure protection and border security, we conducted an experiment under the bilateral Public Security Technical Program between the United States and Canada. It is just one of many efforts by the DHS Science and Technology Directorate to evaluate technologies in a real-world environment and pass on the results to real-world users. Our research was looking for new technology for mobile data encryption across the US-Canada border, to learn whether additional security measures would slow down communications across the borders, and to help first responders tackle their tasks efficiently while keeping their messages secure. We tested four products of interest, including the BlackBerry, and learned a great deal about what does and doesn't work, particularly situations in which messages were delayed, or data were not transmitted.

Another important public-private partnership is Project LOGIIC, which stands for Linking Oil and Gas Industry to Improve Cyber security. The goal is to reduce vulnerabilities in the oil and gas process control system environments. The first demonstration under this project showed how to correlate and analyze abnormal events to identify and prevent cyber security threats.

Project LOGIIC is a model for government-industry technology integration and demonstration efforts to address critical research and development needs. The oil and gas industry contributed the requirements, operational expertise, project management, and product vendor channels. DHS provided the national security perspective on threats, access to long-term security research, independent researchers with technical expertise, and testing facilities. Technology pilot deployments under this program were launched in June of 2006. A planning meeting for the second phase of the LOGIIC partnership took place in March of this year.

Our Directorate also convenes a group called the Identity Theft Technology Council, which meets three times a year to bring together government, venture capital firms, financial sector representatives, academics working in identity theft, and entrepreneurs. Together, we discuss problems, research issues, available technologies, and stay abreast of emerging threats and new opportunities. As a result, venture capital firms and the companies that they fund can connect with government and larger private-sector entities to move emerging security solutions forward. The Council also works closely with the Anti-Phishing Working Group, and has issued two reports: one on phishing and one on malware.

To help technology move out of government research and development, we have sponsored three different types of transition forums:

- At the System Integrator Forum, researchers funded by the DHS Science and Technology Directorate were provided an opportunity to demonstrate their technology to an audience of major system integrators, including Perot Systems/EDS, Northrop Grumman, and General Dynamics, all of whom responded enthusiastically.

- The Emerging Security Technology Forum provided an opportunity for commercial developers to demonstrate their technology to an audience of government early adopters. Our Directorate evaluated 24 commercial technology products to defend against distributed denial of service and worm attacks, and selected 12 for presentation to an audience of government and industry CIOs and potential customers.

- Finally, the IT Security Entrepreneurs Forum -- jointly sponsored with the Kauffman Foundation -- provided small businesses and entrepreneurs an opportunity to learn value propositions and business plan development from the venture capital community and how to open doors into government procurement channels. Chief information officers attended from companies like Sun and Oracle.

The impact of these forums cannot be overstated. They are unique within the federal system. We bring researchers directly to the private sector, so they can demonstrate their technologies in front of more than 100 companies at a time. As I mentioned earlier, this has led to more than 10 commercial cyber security products -- real cyber security solutions that can be widely used by government, industry and citizens around the world. These forums assist projects funded by our Science and Technology Directorate to transfer technology to larger, established security technology companies. Finally, they also help commercial companies provide technology to DHS and other government agencies.

Driving, Discovering and Delivering Cyber Security Solutions: The Path Forward

In the last seven years, more than 20 reports from such entities as the INFOSEC Research Council, the National Science Foundation, the National Institute of Justice, the National Security Telecommunications Advisory Committee, the National Infrastructure Advisory Council, the National Research Council and the President's Commission on Critical Infrastructure Protection have urged the government to do more to drive, discover and deliver new solutions to address cyber vulnerabilities. More recently, academic organizations, such as the Computing Research Association, and industry groups, such as the Cyber Security Industry Alliance and the Internet Security Alliance, also have called for increased funding for cyber security research and development. In addition, the Federal Government has recently produced the Federal Plan for Cyber Security and Information Assurance Research and Development, which includes cyber security R&D priorities of all agencies and departments that participate in the Network and Information Technology Research and Development (NITRD) committee.

To date, I believe that the Department of Homeland Security's Science and Technology Directorate has made excellent progress toward meeting some of the goals outlined in the *National Strategy to Secure Cyberspace*. We need to stay the course and bring these important research and development products into the marketplace. But more needs to be done if we are to counter the negative forces that threaten our cyber security.

Based on the previously cited reports which reflect the views of the professional community and in concert with our customers, the DHS S&T Cyber Security program has identified the following research areas as priorities which we will continue to address in FY2007, FY 2008 and beyond:

- We must continue to advance the development and accelerate the deployment of **more secure versions of fundamental Internet protocols and architectures,** including those for the domain name system and routing protocols described earlier.

- We must improve and create **new technologies for detecting attacks or intrusions,** including monitoring technologies.

- We must improve and create **new methods for mitigation and recovery,** including techniques for containment of attacks and development of resilient networks and systems that degrade gracefully.

- We must develop and support **infrastructure and tools to support cyber security research and development efforts,** including modeling and measurement, test beds, and data sets for assessment of new cyber security technologies, such as the DETER and PREDICT programs I described earlier.

- We must assist the development and support of **new technologies to reduce vulnerabilities in process control systems**.

- We must test, evaluate, and facilitate the transfer of **new technologies associated with the engineering of less vulnerable software and securing the IT software development lifecycle.**

- We need research to identify **new solutions to address malicious software**, such as botnets and other "malware," for which no secure solutions currently exist.

- We must **develop trusted systems**, new hardware and software architectures for security, and **develop cyber security metrics**.

- We must **develop tools that will allow us to visualize network data** so we can see where attacks are coming from and diagnose cyber security problems faster and with more accuracy.

- We must **develop new ways to detect and mitigate insider threats** in cyber security.

- We must develop the **architecture and solutions that will allow us to handle identity management on a wider scale** than is currently possible.

I want to stress for the Subcommittee that research and development involves both promise and progress. The promise lies in our ability to identify threats and potential solutions. But as long as these vital research and development questions remain unanswered, they threaten all of the progress we have made to date, creating weaknesses and vulnerabilities that further complicate our task. The same is true for the areas where we have already made valuable steps forward.

We need to deploy the important infrastructure protections we have helped to develop – across the government and throughout the private sector – and provide incentives for industry to partner in R&D efforts. We need to move forward the already identified next-generation cyber technology research projects that take aim at weaknesses we know today. And we must continue to deliver tested technologies that can become commercially available products, to extend the benefits of our research and offer protection against cyber threats to homes and businesses across the Nation.

The good news, Mr. Chairman and Members of the Subcommittee, is that our research and development efforts show promise in addressing the Nation's cyber security needs. I look forward to working with you to advance our R&D efforts and address the security needs of our Nation's critical infrastructure.

APPENDIX: Selected Major Reports on Cyber Security Research and Development

Biometric Research Agenda: Report of the NSF Workshop. Morgantown, West Virginia, April/May 2003, http://64.233.167.104/search?q=cache:xweu9dx2qMsJ:www.wvu.edu/~bknc/BiometricResearchAgenda.pdf+Biometric+Research+Agenda:+Report+of+the+NSF+Workshop&hl=en&ct=clnk&cd=3&gl=us.

Coordination of Federal Cyber Security Research and Development, U.S Government Accountability Office, GAO-06-811, Sept. 2006, http://www.gao.gov/new.items/d06811.pdf.

Creating a National Framework for Cybersecurity: An Analysis of Issues and Options, Eric A. Fischer, Congressional Research Service, Feb. 22, 2005, http://www.au.af.mil/au/awc/awcgate/crs/rl32777.pdf.

Critical Foundations: Protecting America's Infrastructures. President's Commission on Critical Infrastructure Protection, October 1997, www.fas.org/sgp/library/pccip.pdf.

Critical Information Infrastructure Protection and the Law: An Overview of Key Issues. Computer Science and Telecommunications Board, National Research Council, 2003, http://www.cstb.org/pub_ciip.html.

Critical Infrastructure: Challenges Remain in Protecting Key Sectors, Testimony of Eileen R. Larence, Director, Homeland Security and Justice Issues, and David A. Powner, Director, Information Technology Management Issues, Before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives, U.S. Government Accountability Office, GAO-07-626T, March 20, 2007, http://www.gao.gov/new.items/d07626t.pdf.

Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, Testimony of Robert F. Dacey, Director, Information Security Issues, Before the Subcommittee on Technology Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform, U.S. Government Accountability Office, GAO-04-628T, March 30, 2004, http://www.gao.gov/new.items/d04628t.pdf.

Critical Infrastructure Protection: Challenges in Addressing Cybersecurity, Testimony of David A. Powner, Director Information Technology Management Issues, Before the Subcommittee on Federal Financial Management, Government Information, and International Security, Senate Committee on Homeland Security and Governmental Affairs, U.S. Government Accountability Office, GAO-05-827T, July 19, 2005, http://www.gao.gov/new.items/d05827t.pdf.

Cyber Security Research and Development Agenda. I3P, Dartmouth College, January 2003, http://www.thei3p.org/repository/2003_Cyber_Security_RD_Agenda.pdf.

Electronic Crime Needs Assessment for State and Local Law Enforcement, National Institute of Justice Research Report, March 2001, http://www.ncjrs.org/pdffiles1/nij/186276.pdf.

Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers. Computer Science and Telecommunications Board, National Research Council, 2001, http://www7.nationalacademies.org/cstb/pub_embedded.html.

Hard Problems List. Infosec Research Council. September 1999 (and draft revision as of September 2004) Information Technology Research for Crisis Management. Computer Science and Telecommunications Board, National Research Council, 1999, http://www7.nationalacademies.org/cstb/pub_crisismanagement.html.

High Confidence Software and Systems Research Needs. High Confidence Software and Systems Coordinating Group, Interagency Working Group on Information Technology Research and Development, January 2001, http://www.nitrd.gov/pubs/hcss-research.pdf.

IDs-Not That Easy. Questions About Nationwide Identity Systems. Computer Science and Telecommunications Board, National Research Council, 2002, http://www7.nationalacademies.org/cstb/pub_nationwideidentity.html.

Information Sharing/Critical Infrastructure Protection Task Force Report, National Security Telecommunications Advisory Committee, May 2000, http://www.ncs.gov/nstac/reports/2000/ISCIP-Final.pdf.

Information Technology for Counterterrorism. Computer Science and Telecommunications Board, National Research Council, 2003, http://www7.nationalacademies.org/cstb/pub_counterterrorism.html.

Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, Michelle Keeney, Dawn Cappelli, et al, Carnegie Mellon Software Engineering Institute, May 2005, http://www.cert.org/cert/work/organizational_security.html.

Internet Domain Names: Background and Policy Issues, Lennard G. Kruger, Congressional Research Service, Sept. 22, 2005, http://www.au.af.mil/au/awc/awcgate/crs/97-868.pdf.

The Internet Under Crisis Conditions: Learning from September 11. Computer Science and Telecommunications Board, National Research Council, 2003, http://www7.nationalacademies.org/cstb/pub_internet911.html.

National Security Telecommunications Advisory Committee, Research and Development Exchange Workshop, Atlanta, Georgia, March 2003, http://www.ncs.gov/nstac/rd/nstac_03_bos.html.

National Security Telecommunications Advisory Committee, Research and Development Exchange Workshop. Tulsa, Oklahoma, September 2000, http://www.ncs.gov/nstac/reports/2001/R&D_Exchange2000Proceedings.htm.

National Security Telecommunications Advisory Committee, Research and Development Exchange Workshop. West Lafayette, Indiana, October 1998, http://www.ncs.gov/nstac/reports/1998/R&DExchange.pdf.

National Strategy to Secure Cyberspace, The White House, February 2003, http://www.whitehouse.gov/pcipb/.

Protecting Systems Task Force Report on Enhancing the Nation's Security Efforts, National Security Telecommunications Advisory Committee, May 2000, http://64.233.167.104/search?q=cache:JkJUKZ9OmYsJ:www.ncs.gov/nstac/reports/2000/PSTF-Final.pdf+Protecting+Systems+Task+Force+Report+on+Enhancing+the+Nation%E2%80%99s+Security+Efforts,+National+Security+Telecommunications+Advisory+Committee,+May+2000,&hl=en&ct=clnk&cd=1&gl=us.

Robust Cyber Defense. Study commissioned for DARPA ITO, Fall 2001. Slides available at: http://www.cs.cornell.edu/fbs/darpa.RobustCyberDefense.ppt.

Technology Assessment: Cybersecurity for Critical Infrastructure Protection, U.S. Government Accountability Office, GAO-04-321, May 2004, http://www.gao.gov/new.items/d04321.pdf.

Trust in Cyberspace. Computer Science and Telecommunications Board, National Research Council, 1999, http://books.nap.edu/readingroom/books/trust/.

Understanding the Insider Threat, Richard C. Brackney, Robert H. Anderson, Conference Proceedings of a March 2004 Workshop, RAND, National Security Division, http://www.rand.org/pubs/conf_proceedings/2005/RAND_CF196.pdf.

Who Goes There? Authentication Through the Lens of Privacy. Computer Science and Telecommunications Board, National Research Council, 2003, http://www7.nationalacademies.org/cstb/pub_authentication.html.

Workshop on Scalable Cyber-Security Challenges in Large-Scale Networks: Deployment Obstacles. Large Scale Networking Coordinating Group, NITRD, Landsdowne, Virginia, March 2003, http://64.233.167.104/search?q=cache:mWKvtoq_xLoJ:cs.yale.edu/homes/jf/LSN-report.pdf+Workshop+on+Scalable+Cyber-Security+Challenges+in+Large-Scale+Networks:&hl=en&ct=clnk&cd=1&gl=us.